Les fondamentaux de la cybersécurité

DOMAINE : *Les essentiels*
CATEGORIE : *Fondamentaux*

MISE A JOUR LE 11/02/2025

Descriptif

Cette formation vous offre une **introduction complète** aux principes essentiels de la **cybersécurité**. Vous découvrirez les **menaces** courantes telles que les malwares, le phishing et les attaques par déni de service, ainsi que les meilleures **pratiques** pour **protéger** vos données et systèmes.

Ce programme couvre également les **concepts** de base **techniques et organisationnels** en matière de sécurité de l'information.

À travers des **exemples concrets** et des exercices pratiques, vous apprendrez à **identifier** les vulnérabilités, mettre en place des **mesures de sécurité** et à développer une stratégie de réponse aux **incidents**.

Cette formation est **idéale** pour toutes personnes souhaitant acquérir des **compétences solides** en cybersécurité.

Informations

Référence	**CY-FCYB-FSEC**

Publics concernés

Toute personne souhaitant approfondir ses connaissances en cybersécurité

Formateur

Expert certifié en cybersécurité

Prérequis

Avoir des connaissances de base en technologie de l'information

Certification préparée

Aucune

Objectifs

- Comprendre et savoir **appliquer** les concepts de base de la **cybersécurité**.
- Comprendre les environnements **techniques et organisationnels** liés à la cybersécurité.
- Savoir mettre en place des **mesures de sécurité**.
- Savoir réagir face aux **incidents de sécurité**.
- Être initié aux **normes de sécurité**.

Type de session

Intra-entreprise, **inter-entreprise** (en présentiel ou à distance)

Durée	5 jours (35 heures)
Date	À la demande
Tarif	2.050 € H.T
Effectif	12 participants max
Niveau	**Intermédiaire**
Délai d'accès	**3 semaines**

Programme

1) Introduction à la cybersécurité

- Le monde de la cybersécurité
- Les principaux termes et définitions
- La confidentialité, de l'intégrité et de la disponibilité
- Les différents acteurs de la sécurité
- L'importance de la cybersécurité
- Les métiers de la cybersécurité

2) Les principales menaces

- Différences entre menaces et vulnérabilités
- L'ingénierie sociale
- Présentation des attaques les plus courantes
- Les différents types de logiciels malveillants
- Les méthodes de protection
- Le rôle de l'IA

3) La sécurité organisationnelle

- L'importance des politiques de sécurité
- Etablissement des rôles et des responsabilités
- Les processus de gestion des incidents
- Savoir communiquer, à qui et comment

4) La sécurité technique

- La sécurité des actifs physiques et numériques
- Les systèmes d'exploitation et la sécurité
- Les techniques de chiffrement et de hachage
- Introduction aux certificats et aux PKI
- La dissimulation des données

Ce programme peut être adapté pour des sessions plus courtes, plus longues ou selon des besoins spécifiques

5) La sécurité des réseaux

- Présentation des architectures réseau
- Les principales attaques sur les réseaux
- Vulnérabilités des réseaux sans fil
- Scanner et analyser le trafic réseau
- Les concepts de sécurité des réseaux
- Les outils de protection logiciels et matériels

6) La sécurité applicative

- L'analyse statique et dynamique du code
- L'intégration et le déploiement continue
- La sécurité des applications mobiles (IoT)
- Intégration de la sécurité dans le SDLC

7) La sécurité web

- Les attaques les plus courantes
- Protocoles sécurisés, cookies et sessions
- Protection des applications web
- Le Framework OWASP

8) Introduction aux tests d'intrusion

- Principe de fonctionnement et méthodologie
- Les techniques de hacking éthique
- Construire et restituer le rapport de sécurité

9) La réponse aux incidents de sécurité

- Détection des intrusions
- Analyser les événements
- Initiation au forensiques
- Les outils de gestion des crises de sécurité

10) Les normes de sécurité

- Notions de conformité
- Objectifs des normes
- Les normes de la famille 27000
- Initiation aux audits de sécurité

11) Projet pratique

- Présentation du laboratoire virtuel
- Présentation du Framework MITRE ATT&CK
- Simulation attaquants / attaqués
- Evaluation et rétrospective collective

Modalités pédagogiques

Nous mettons en œuvre des modalités pédagogiques **variées** afin de maintenir l'attention des participants. Cette formation s'appuiera sur :

- Une alternance théorie (35%) et pratique (55%).
- Des mises en situation réelle, études de cas et échanges de pratiques.
- Des mises à disposition d'outils numériques interactifs, collaboratifs et participatifs.

À la fin de la formation, toutes les ressources pédagogiques seront **mises à disposition** pour tous les participants via leur espace dédié.

Modalités d'évaluation et de suivi

Les acquis de l'action de formation sont **évalués** à partir des productions des participants lors des études de cas et à partir de quiz et exercices réguliers.

Un questionnaire **d'autoévaluation** au regard des objectifs de la formation vous sera transmis avant le début de la formation et à la fin de celle-ci, vous permettant ainsi de mesurer votre progression en fin de formation.

Information sur l'accessibilité

Nous remercions les personnes qui auraient des **besoins spécifiques** de nous le signaler dès leur inscription. Quel que soit le type de handicap, nous pouvons adapter certaines de nos modalités de formation en étudiant ensemble vos besoins. Pour toutes questions, merci de contacter notre **référent handicap** :

- Par mail à handicap@ghdeformation.fr
- Ou par téléphone au +33 06 78 84 71 24